



CYBERPAX

Make sure your SOC team is prepared for zero-day, even if they have never experienced it.

Training Outline

SOC Intrusion - Detection Tactics

CybergymIEC's SOC Intrusion – Detection Tactics training challenges your cybersecurity team with a real-life, dynamic cyberattack that will force them to pull together as they work to protect your organization.

Your experts will be put through their paces at one of our cyberwarfare arenas - a secure training facility, where our team of professional Red Hat hackers attempt to infiltrate 'your systems' in a series of cyberattacks, run on a real-life technological environment. Through a series of hands-on exercises, your team will have to work together and think on their feet as they develop the essential skills required to anticipate and prevent a cyberattack.

Over the course of the training, participants will master rule configuration and data correlation to optimize their SIEM systems, all under live cyber-incident conditions.



Participants

- SOC Analysts
- Incident Response Team Members
- IT/OT Professionals



Prerequisites

- Basic knowledge of SIEM operation and configuration
- Good understanding of data communications
- Understanding of basic information security concepts and tools



Training Outcomes

- Ability to detect and analyze intrusions and data breaches
- Enhanced skills for SIEM configuration and optimization
- Insight into the hacker's perspective



Duration

- 24 hours (3 x 8-hour days)

#SecurityExperts

#SIEM

#SOCIntrusion

#Detecting